公開キー方式の暗号

新潟県立新発田高等学校　金沢光則

平成 13 年 6 月 10 日

1　はじめに

次のようなメールをいただきました。

> あるホームページに「電子署名・認証の仕組み」が簡単に説明されていました。あいうえお … に 1,2,3,4,5,$\cdots$ と対応させて公開鍵と秘密鍵の説明をしていました。たとえば「し」は 12 が対応しますが、$12\times12\times12=1728$, これを 55 で割ったあまりは 23 で「ぬ」。この 23 を 7 回かけて（$23^7=3404825447$），これを 55 で割ったあまりは 12 で「し」。「し」を「ぬ」にする過程が暗号化で、$\{3,55\}$ が公開鍵,「ぬ」を「し」に戻すところ（復号）の $\{7,55\}$ が秘密鍵というのだそうですが、式で書くと $a^3=55m+r$, $r^7=55n+s$ (上の例では $a=12$, $r=23$, $s=12$, m, n は商で整数) のとき $a=s$ ということになりますが、簡単に示せますか？出所は http://www.jipdec.or.jp/easc/esac.htm です。

解説は情報系でよく見るのですが，簡単な数学上のポイントをまとめてみました。

2　孫子の剰余定理とフェルマーの小定理

2.1　孫子の剰余定理

任意の a, b に対して，$x\equiv a(\mod 5)$, $x\equiv b(\mod 11)$ を満たす x が　mod 55 でただ 1 つ存在する。

2.2　フェルマーの小定理

素数 p に対して，$a\neq0(\mod p)$ ならば $a^{p-1}\equiv1(\mod p)$ が成り立つ。

2.3　質問の回答

フェルマーの小定理から
$(a^3)^7=a^{21}=(a^5)^4\times a\equiv a(\mod 5)$.
$a^{21}=(a^2)^{10}\times a\equiv a(\mod 11)$.
よって孫子の剰余定理から $a^{21}=a(\mod 55)$ が成り立つ。

2.4　3 と 55 から 7 を求める

$3k\equiv1(\mod 4)$, $3k\equiv1(\mod 10)$ となるような k を見つければよい。
このためには，$3k-1=4\times5$ とおけばよく，このとき，$k=7$ となる。

3 実際の場合

暗号用のキー a , 2 つの素数の積 pq を公開する。このとき，p, q は同程度の桁数を持つ非常に大きな素数とする。積から素因数分解により p, q を求めることが出来れば，復号用のキー b を計算することができ，暗号の役目を果たさないが，実際には素因数分解には非常に長い時間がかかり，実際には不可能に近い。この事実上不可能であるということに，公開暗号キー方式は依っているのである。
わざわざ知らせることもないので，公開する必要はないが，知られても良いということである。しかし，積極的に公開キーを使えば，署名をすることができる。復号キーを使って暗号化すれば，誰でも署名部分を暗号キーを使って復号することができ，しかも，それができるのは，復号キーを知っている本人だけだということになるからである。

3.1 孫子の剰余定理

一般には，次の同型が成り立つ。ただし，$p_1, p_2, \cdots, p_n$ は互いに素とする。

$$\mathbb{Z}/pq\mathbb{Z} \ni \overline{a} \rightsquigarrow (\overline{a}, \cdots, \overline{a}) \in \mathbb{Z}/p_1\mathbb{Z} \times \cdots \mathbb{Z}/p_n\mathbb{Z}$$

3.2 復号キーの作り方

r を与えたとき，$(a^r)^k \equiv a(\mod pq)(\forall a)$ が成り立つ k を求めたい。
$rk \equiv 1(\mod p-1), rk \equiv (\mod q-1)$ となる k を作ればよい。
$(r,(p-1)(q-1)) = 1$ なら，$rk + (p-1)(q-1)y = 1$ となる整数 k,y が存在する。
$0 < k < (p-1)(q-1)$ として良いから，この k を復号キーに使えばよい。特に，r が素数なら，常に復号キーは存在する。
$p = 5, q = 11, r = 3$ のときに実行してみると，
$40 = 3 \times 13 + 1 \therefore 3 \times (-13) + 40 = 1 \therefore 3 \times (-13 + 40) + 40 \times (1 - 3) = 1 \therefore 3 \times 27 \equiv 1(\mod 40)$
$\therefore 3 \times 27 \equiv 1(\mod 4), (\mod 10)$
4, 10 の最小公倍数を使って計算すれば，$20 = 3 \times 6 + 2, 3 = 2 \times 1 + 1$ だから，$3 = (20 - 3 \times 6) \times 1 + 1$
$\therefore 3 \times 7 + 20 \times (-1) = 1 \therefore 3 \times 7 \equiv 1(\mod 20) \therefore 3 \times 7 \equiv 1(\mod 4), (\mod 10)$